

ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM POLICIES FOR Decode Global LTD AS OF February 26th 2024

INTRODUCTION

a. Objective

- i. This document sets out the Money Laundering (AML)/ Counter Financing of Terrorism (CFT) Policy for Decode Global LTD (hereinafter referred to as "The Company") to comply with International Anti-Money Laundering and Anti-Terrorism Financing rules and practice the Financial Action Task Force's recommendation. It is intended to ensure that the institution understand and comply with the requirements and obligations imposed to them.
- ii. The Company does not permit the use of our brokerage service for Money Laundering and Terrorist Financing purposes.
- iii. This document is also formulated to ensure that all The Company's employees understand and comply with the requirements and obligations imposed to them.
- iv. For awareness, training, and education purpose.

DEFINITIONS

a. What is Money Laundering

Money Laundering encompasses all activities, procedures or processes aimed to legitimize funds obtained through illegal or criminal activities. The brokerage services provided might serve as an avenue to launder money. The use of the money brokerage industry legitimates the proceeds of crime would also threaten the integrity, trust, and confidence of the public in the industry itself. In the bigger scheme of things, money laundering would bring dire social and economic consequences.

b. Stages of Money Laundering

i. Placement

In the initial or placement stage of money laundering, the criminal introduces his illegal profit and ill-gotten gains into the financial system. This is the physical disposal or dealing of the initial proceeds derived from illegal activities.

ii. Layering

After the funds have entered the financial system, the "layering stage" takes place. In this phase, the illicit proceeds are separated from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide an appearance of legitimacy as well as anonymity.

iii. Integration

When layering succeeds, the criminal proceeds have been successfully laundered, i.e., cleaned and are regarded for all intent and purposes as legitimate funds and are then reintroduced, i.e., integrated back into the financial system through investment in business, purchase of assets.

c. What is Financing Terrorism

- i. Financing of terrorism refers to carrying out transactions involving funds that may or may not be owned by terrorist, or that have been, or are intended to be, used to assist the commission of terrorism.
- ii. In the financing of terrorism, the focus is on the determination or use of funds, which may have been derived from legitimate sources.

1. AML and CTF Risk Assessment

- 1.1. This AML & CTF Program sets risk assessment process which is grounded on risk-based approach.
- 1.2. The main components of the risk assessment process are:
 - 1.2.1. Risk identification,
 - 1.2.2. Management and mitigation of risks, and
 - 1.2.3. Risk assessment reporting.
- 1.3. In identifying ML/TF risks, The Company has considered the risk posed by the following risk factors:
 - 1.3.1. our customer types, including any Politically Exposed Persons;
 - 1.3.2. the types of services we provide;
 - 1.3.3. the methods by which we deliver our services;
 - 1.3.4. the foreign jurisdictions with which we deal; and
 - 1.3.5. the business structure and process.
- 1.4. The risk assessment will provide the foundation for
 - 1.4.1. The categorization of customers into different due diligence levels within the KYC process, and
 - 1.4.2. The identification of situations and cases where monitoring and/or other additional risk mitigation measures will be required.

2. Risk Factors Considered

certain customer types, services, delivery methods, foreign jurisdiction considerations and business structures and processes can pose a higher ML/TF risk. At a high-level, risk factors that we may reasonably face are identified as follows:

- 2.1. **Customer Type:**
 - 2.1.1. The customer identity, origin of wealth or source of funds cannot be easily verified;
 - 2.1.2. Where the structure of the customer/entity renders it difficult to identify the true controlling owner, or where there is no legitimate commercial rationale for the structure;
 - 2.1.3. The customer is a Politically Exposed Persons ("PEP");
 - 2.1.4. Customers engaged in a business which involves the physical handling of significant amounts of cash (e.g., currency exchange bureau, money transmitters, dealers in high value goods, on-line auction sites, casinos, betting, and other gambling related activities who routinely receive payment in cash);
 - 2.1.5. Customers who appear on governments lists, including sanction lists, or other credible sources which trigger risks in respect of corruption and/or criminal activity;
 - 2.1.6. Customers (not necessarily PEPs) based in, or conducting business in or through, a high-risk geographic location, or a geographic location with known higher levels of corruption or organized crime, or drug production/distribution;
 - 2.1.7. Charities and other "not for profit" organizations which are not subject to some form of regulatory monitoring or supervision.
 - 2.1.8. Professional service providers such as lawyers, accountants, investment brokers or other professionals holding accounts for their customers or acting on behalf of their customer and where we would be required to place an unreasonable reliance on the professional service provider;
 - 2.1.9. Requests for undue levels of secrecy with a transaction;
 - 2.1.10. Whether the customer is a long-standing customer or undertakes occasional

transactions;

- 2.1.11. The customer's business activities place the customer in a high-risk category (military industry, casino etc.)

2.2. **The Types of Services Provided**

The Company is a company structured to electronic trading and brokerage services for on financial products to retail and wholesale clients. Although not necessary, certain products, services, and transactions in relation to them may pose a higher risk. E.g., the following products and services may pose a high risk under certain circumstances:

- 2.2.1. Services where large amounts are invested;
- 2.2.2. Services involving structures intended to (or which can in practice) render a customer anonymous (e.g., accounts in the names of trusts or nominees of third persons);
- 2.2.3. Services whereas the client trades for no apparent speculation, arbitrage or hedging purpose.
- 2.2.4. Services where the client intends to trade at conditions (e.g., fees) that are clearly unfavorable to him/her.

2.3. **The methods by which we deliver our services.**

Products and services provided in a non - face to face process, i.e., when the customer has not been physically present for identification purposes may pose higher risks.

2.4. **Foreign Jurisdictions**

Customers based in, or conducting business through certain countries may pose a higher risk. Criteria for identifying high risk countries are e.g.:

- 2.4.1. Countries identified by credible sources as providing funding or support for terrorist activities or who have terrorist groups working within the country;
- 2.4.2. Countries subject to sanctions and embargoes by the United Nations;
- 2.4.3. Countries identified by credible sources as having significant levels of corruption and/or criminal activity;
- 2.4.4. Countries identified by credible sources as lacking appropriate AML and CTF legislation;
- 2.4.5. Countries identified by the FATF as non-co-operative countries and territories.

2.5. **Business Structure and Process**

The Company's simple organizational and business structure as well as clearly defined business and operational processes allow to define AML and CTF risk according to this criterion as low.

3. **Management and mitigation of risks**

- 3.1. Based on the risk assessment foundation, the following measures shall be applied:
 - 3.1.1. Assigning risk level (low, medium, or high) to all customers, based on the risk assessment foundation,
 - 3.1.2. Applying enhanced due diligence measures to high-risk customers,
 - 3.1.3. Increasing staff awareness and knowledge of AML and CTF and The Company's measures to prevent it (e.g., through frequent/deeper staff training),
 - 3.1.4. Monitoring of customers' activities and transactions, carried out manually by the client relationship manager within ongoing customer due diligence, and electronically by AML and CTF Compliance Officer(s),

- 3.1.5. Escalating the decision regarding establishment of a relationship in the case of a high-risk customer, or (where appropriate) carrying out of a specific action, including procedures for the rejection or termination of customer relationships, and
- 3.1.6. Reviewing and amending AML and CTF processes and routines.

3.2. Whenever a certain risk is identified that needs mitigation, risk mitigation measures shall be considered and implemented in relation to each of new and existing customers, and new and existing products and services. If the identified risks cannot be mitigated immediately, an action plan shall be established.

4. Compliance function in AML and CTF

4.1. The Company has established compliance function within the Company directly reporting to the Board of Directors, led by Chief Compliance Officer, and having specifically dedicated staff as AML&CTF Compliance Officers.

4.2. Responsibilities of AML and CTF Compliance Officer(s):

- 4.2.1. monitoring compliance and adherence to the obligations of the AML and CTF Act;
- 4.2.2. receiving and investigating reports of suspicious matters activities;
- 4.2.3. adopting a risk-based approach to monitoring customer activity to identify suspicious activity;
- 4.2.4. ensuring that proper AML and CTF records are maintained;
- 4.2.5. reporting suspicious activity to FIU;
- 4.2.6. providing advice to Representatives;
- 4.2.7. receiving and carrying out directions or orders issued by Chief Compliance Officer and/or Authorities; and
- 4.2.8. liaison with the VFSC (Vanuatu Financial Services Commission), VFIU (Vanuatu Financial Intelligence Unit), and other regulatory bodies and law enforcement in respect of suspicious activity and threshold reporting.

4.3. AML and CTF related responsibilities of Chief Compliance Officer(s):

- 4.3.1. preparation and review of AML Policy and Program;
- 4.3.2. overseeing communication and training for employees;
- 4.3.3. providing advice to AML&CTF Compliance Officers and other Representatives;
- 4.3.4. submitting reports to the Board (at least annually);
- 4.3.5. lodging annual compliance report with Authorities;
- 4.3.6. receiving and carrying out directions or orders issued by Authorities; and
- 4.3.7. liaison with VFSC, VFIU, and other regulatory bodies and law enforcement in respect of suspicious activity and threshold reporting.

4.4. Chief Compliance Officer as well as AML and CTF Compliance Officer(s) are authorised and have full capacity to act independently in order to fulfil the commitments of his/her role as well as receive all information necessary to carry out the compliance functions from the Representatives.

4.5. The compliance function must be consulted prior to The Company: introducing a new designated service to the market; introducing new methods of delivery of a designated service; and/or introducing any new or developing technology used for the provision of designated services to enable the AML and CTF Compliance Officer(s) to identify any significant changes in ML/TF risks and to formulate controls to mitigate

and manage those risks.

- 4.6. The Company appointed two fit and proper natural persons to carry out the functions of Compliance Officer, also acting as MLRO (Money Laundering Reporting Officer), and an Alternate Compliance Officer.
- 4.7 The Alternate Compliance Officer shall assist the Compliance Officer to carry out his/her functions under this Policy and shall replace and assume the interim of the Compliance Officer whenever he/she is unavailable to carry out such functions.
- 4.8 The names of the Compliance Officer and the Alternate Compliance Officer are mentioned in the table at the end of this Policy.

5. Risk assessment reporting

- 5.1. It is the responsibility of AML&CTF Compliance Officers to report suspicious activity or transactions and file incident reports to the Authorities as well as keep the Chief Compliance Officer informed on the everyday basis about all AML and CTF issues, defaults, or incidents.
- 5.2. Chief Compliance Officer shall, on an ongoing basis, inform the Managing Director and the Board of Directors of the material events related to management and mitigation of Money Laundering risks in The Company.
- 5.3. The relevant reported AML and CTF related information is included in an annual compliance report prepared by the Chief Compliance Officer and presented to the Board of Directors. The report shall contain information on incidents and/or outlined areas that need improvement and where there are deficiencies or proposals for improvement, a plan showing how these are to be handled.
- 5.4. Records shall be kept of all reports in accordance with general record keeping principles.

6. AML and CTF Training Program

- 6.1. Appropriate training with regard to money laundering and terrorist financing is vital in managing the ML/TF risk. Accordingly, all Representatives of The Company are required to undergo training in AML and CTF laws and The Company's internal policies. In order for our ML/TF controls to be successful, training programs are formulated having regard to the representative's level of responsibility and position.
- 6.2. Updated or refresher training will depend upon staff promotions and/or depending upon the level of assessed ML/TF risk of the designated service.
- 6.3. The training can be internal or external (by contracted training organisations). Specific AML and CTF related external training would be available to certain Representatives according to their responsibilities (such as Chief Compliance Officer, AML/CTF Compliance Officers etc.). It is a responsibility of Chief Compliance Officer to arrange internal training. Ongoing training will occur on a periodic basis.
- 6.4. At a minimum the AML and CTF training program will be designed to enable Representatives to understand the following:

- 6.4.1. the AML and CTF Policy;
 - 6.4.2. the AML and CTF Program;
 - 6.4.3. the obligations of The Company under the AML and CTF Act and underlying legal requirements;
 - 6.4.4. the types of ML/TF risk The Company might face and the potential consequences of such risks;
 - 6.4.5. how to identify signs of ML/TF that arise during the course of carrying out their duties;
 - 6.4.6. escalation procedures i.e., what to do once a ML/TF risk is identified;
 - 6.4.7. what employees' roles are in the firm's compliance efforts and how to perform them i.e., the processes and procedures relevant to each person's role;
 - 6.4.8. the company's record keeping and record retention policy; and
 - 6.4.9. the consequences (including civil and criminal penalties) for non-compliance with the AML and CTF Act and supporting Rules.
- 6.5. Records of training must be maintained to demonstrate that the person/s attended the training session/s, the dates of training, a brief description of the subject matter of the training provided and the number of hours (or level of accreditation) for attending the course/session/seminar.
- 6.6. Training frequency:
- 6.6.1. Annually: All employees dealing with client-related matters or, who, due to the nature of their position, have special needs of AML knowledge, shall undergo training, be updated and/or informed regarding important and relevant AML regulations and relevant internal procedures as appropriate. All newly on boarded Representatives shall undergo training within 3 (three) months.
 - 6.6.2. Ongoing: For employees operating in areas which may represent high risk, e.g., correspondent banking, the need for tailor made training or information shall continuously be assessed by Chief Compliance Officer in collaboration with the business, and when a need is identified, action shall be taken.

7. Monitoring process and Suspicious Matter Reporting

- 7.1. The Company has implemented Transaction Monitoring process defined herein which includes appropriate risk-based systems and controls to scrutinize transactions that are inconsistent with information held about the business relationship with the reporting entity. The transaction monitoring system is set to identify any transaction that appears to be suspicious, complex, unusual and have no apparent visible economic or lawful purpose;
- 7.2. The Company has also implemented Customer Monitoring Process where it monitors its relationship with its customer ensuring that the customer's activities being conducted are consistent with The Company's knowledge of the customer, the customer's business, source of funds and risk profile;
- 7.3. Customer activities and transactions shall, based on a risk-based approach, be monitored by the client relationship manager within day-to-day activities and within ongoing customer due diligence and electronically by AML and CTF compliance Officer(s). Any and every payment that would not fall within the expected payments associated with certain clients should be singled out and further examined by the AML/CTF Compliance Officers.

- 7.4. All monetary transactions and related data (accounts, involved parties and relations) are to be individually and manually reviewed and their purpose verified by the document substantiating the purpose of the transaction (contracts, invoices, loan agreement etc.). This requirement may be exempted in cases of small amount transactions or otherwise due to risk-based approach applied in the Company. Furthermore, every incoming and outgoing payment has to be filtered through the World Check's sanctions lists and/or any other reliable sources available to the Representative at the moment.
- 7.5. The initial or ongoing due diligence and monitoring may give rise to concerns requiring a review. The following are examples of circumstances which may give rise to such concerns:
- 7.5.1. Refusal to disclose details concerning business activities, e.g., unwillingness to disclose the source of funds or wealth or unwillingness to provide names of and other information on owners and other people with significant control over the business entity,
 - 7.5.2. The behavior of the customer diverges from previous pattern or stated pattern, e.g., an inactive account suddenly becomes active with large transactions,
 - 7.5.3. A prospective customer promises a trading volume, which does not make economic sense in the light of his background and other activities,
 - 7.5.4. The purpose and intent behind the transaction or relationship is unclear, e.g., when the commercial rationale for certain service is missing or weak,
 - 7.5.5. The representative suspects on reasonable grounds that the customer is not the person they claim to be or that the customer's agent is not the person they claim to be,
 - 7.5.6. The Representative suspects on reasonable grounds that the provision, or prospective provision, of the service is preparatory to the commission of an offence of financing of terrorism.
- 7.6. The assessment as to what constitutes suspicion shall be based on the information about the client received by the Representative handling the matter, and the scope of the client's business, along with the Representative's general knowledge of deviating or suspicious transaction or activity patterns.
- 7.7. If the result of a review gives rise to an actual or potential suspicion related to Money Laundering the Representative shall immediately report the issue to compliance function, which shall initiate an investigation and decide whether to report the issue to the FIU. Matters of a more serious nature where a report to FIU has been filed shall be reported to the Board of Directors.
- 7.8. AML/CTF Compliance Officer(s) are responsible for the reporting to FIU.
- 7.9. Detailed suspicious matter reporting requirements are set in AML&CTF Act Part 6 and include:
- 7.9.1. obligation to report suspicious transaction (STR);
 - 7.9.2. obligation to report suspicious activity (SAR);
 - 7.9.3. obligation to report transaction conducted by prescribed entities (as defined in AML&CTF Act Rules Article 11);
 - 7.9.4. obligation to report transaction involving terrorist property;

- 7.9.5. obligation to report certain transaction with no legitimate purpose;
- 7.9.6. other reporting obligations which may or may not be connected with suspicions in ML/TF activities and include obligation to report international currency transfers (above 1000000 VT or equivalent in foreign currency), obligation to report large cash transactions (not applicable to The Company since no cash transactions are allowed).
- 7.10. The procedure for suspicious matter reporting is described below.
- 7.11. Suspicious Transaction Report (**STR**) is to be filed **on a transaction** or attempted transaction regarding which The Company suspects or has reasonable grounds to suspect that it involves proceeds of a crime, relate to terrorist financing, is complex, unusual, or large, and does not have any apparent visible economic or lawful purpose.
- 7.12. In slight contrast a Suspicious Activity Report (**SAR**) shall be reported on a **series of transactions** and/or attempted transactions (which form a pattern or trend) which The Company suspects or has reasonable grounds to suspect to involve proceeds of crime or is related to terrorist financing.
- 7.13. It is important that any attempt to overcome the threshold requirements by conducting 2 or more transactions below the prescribed threshold amounts with the purpose to avoid the reporting has been identified, investigated and where necessary reported to the authorities.
- 7.14. Reports filed with FIU on suspicious Money Laundering or financing of terrorism shall be recorded and kept according to requirements set out in this Program.
- 7.15. It is prohibited to disclose to the customer concerned or to other third persons outside The Company the fact that a report has been filed or that a Money Laundering investigation is being or may be carried out.
- 7.16. The Company must take all appropriate measures to protect Representatives who report suspicious activity from being exposed to threats or hostile action.
- 7.17 In Compliance with Part 3 of the United Nations Financial Sanction Act No.6 of 2017 ("UNFS Act") and subsequent amendments, the Company shall ensure that:
- 7.17.1. it has properly identified the ultimate beneficial owner of any company, or other property that is involved in a deal carried out by the Company.
- 7.17.2. it does not deal with a property that is known or that can be reasonably suspected to be owned, controlled or held, directly or indirectly, wholly or jointly, by or on behalf of or at the direction of a person or entity (hereinafter referred to as a "Designated Person or Entity") subject to sanctions or in any case a person or entity designated by the United Nations Security Council or its Committees pursuant to the Resolutions listed in Schedule 1 of the UNFS Act, or prescribed by Regulations referred to in section 3 of the UNFS Act, or designated by the Prime Minister of the Republic of Vanuatu under section 4 of the UNFS Act.
- 7.17.3 it does not make property or a financial service available directly or indirectly, wholly or jointly, to Designated Person or Entity,
- 7.17.4. the identity and details of all its clients and potential clients are scanned and

checked upon first onboarding and periodically every 12 months, against the United Nations Financial Sanctions List, as well as other international sanctions lists.

8. Record Keeping.

- 8.1. In accordance with meeting legislative obligations, The Company will retain all records relevant to its AML and CTF Program and policies, including the following:
 - 8.1.1. the AML and CTF Program and all reviews and addendums to the same;
 - 8.1.2. its AML and CTF Policy and all reviews and addendums to the same;
 - 8.1.3. transactional records;
 - 8.1.4. Customer identification and verification records;
 - 8.1.5. Audits and compliance reviews;
 - 8.1.6. Suspicious matter and other reports made to FIU;
 - 8.1.7. All enquiries relating to ML and TF made to The Company by the FIU or law enforcement agency;
 - 8.1.8. Management approvals;
 - 8.1.9. Customer account/relationship records;
 - 8.1.10. Annual compliance reports and other management reports;
 - 8.1.11. Training and compliance monitoring reports; and
 - 8.1.12. Information relating to the effectiveness of training.
- 8.2. Records in respect of customer identification and verification are to be retained for 6 years after account closure.
- 8.3. Where The Company (or its agent or intermediary) carries out a customer identification and verification procedure with respect to a prospective customer to whom The Company proposes to provide a service, it must make (and retain) a record of:
 - 8.3.1. the procedure (i.e., the Checklist); and
 - 8.3.2. information obtained in the course of carrying out the procedure (i.e., supporting documentation to verify the identification of the customer); and
 - 8.3.3. such other information (if any) about the procedure as is specified in the AML and CTF Act.
- 8.4. Records in respect of financial transactions are to be retained for 6 years after the date of the transaction.
- 8.5. AML and CTF Program and addendums together with any documentation relevant to the reason for amendment are also to be retained for 6 years after the adoption of the AML and CTF Program and/ or amendments cease to be in force.

9. Financial Intelligence Unit (FIU) Feedback

- 9.1. FIU is the main AML and CTF regulator. FIU's role is to monitor The Company's compliance with the AML/CTF legislation.
- 9.2. FIU may provide The Company with feedback in respect of its performance on the management of ML/TF risk. FIU also has the power to compel licensees to produce certain information.
- 9.3. The receipt of any notice, direction, or recommendation from FIU will be immediately referred to the AML and CTF Compliance Officer.

- 9.4. Notices from FIU may include the following:
- 9.4.1. to compel production of information or documents;
 - 9.4.2. to enter premises under a monitoring warrant;
 - 9.4.3. to require an external audit or AML and CTF risk assessment;
 - 9.4.4. to provide remedial direction; and
 - 9.4.5. to accept enforceable undertakings.
- 9.5. The Chief Compliance Officer as well as AML and CTF Compliance Officer(s), in conjunction with other Representatives, will take all steps necessary to comply with any feedback, notices, orders, warrants etc. or to implement any directions issued by FIU.
- 9.6. The AML and CTF Compliance Officer will prepare appropriate reports for FIU. Reports required by law or by FIU will be forwarded within the period specified in such law or any notice or order or if FIU allows a longer period, that longer period.
- 9.7. The Chief Compliance Officer as well as AML and CTF Compliance Officer(s) will have due regard to any feedback provided by FIU in respect of The Company's performance in managing its ML/TF risks. Such feedback will be incorporated into ongoing monitoring programs and the AML and CTF Program will be amended (where appropriate).
- 9.8. The Chief Compliance Officer will be responsible for the implementation of any specific recommendations made by FIU to The Company in respect of its ML/TF risk management performance.
- 9.9. The AML and CTF Compliance Officer(s) will monitor FIU information sources, circulars, and guidance notes, in respect of domestic and international issues which may affect the business. This includes financial sanctions and updates to lists of terrorist groups.

10. Independent review of AML and CTF Program

- 10.1 The Company shall appoint a professional to carry out periodic audits of its AML & CFT procedures. For this purpose, the Director of the Company will select and engage an independent professional that has relevant experience in the financial services industry as well as the AML/CFT function and international regulations.
- 10.2 The AML/CFT audit shall be conducted within 3 months from the last day of the license renewal month of The Company, and it shall cover the activity carried out during the period (hereinafter referred to as the "AML/CFT audit period") starting on the first day of the month after either the issue date of the license or the previous renewal date, whichever is the latter, and ending on the last day of the month of the latest renewal date. (e.g. for a company with license issue/previous renewal on the 10th of March 2020 and latest renewal on the 10th of March 2021, the "AML/CFT period will cover the period 1st of April 2020 to 31st March 2021).
- 10.3 The Compliance Officer and/or the Alternate Compliance Officer will be involved in the audit process on the Company side and will be responsible, inter alia, for filling out the pre-audit questionnaire provided by the Auditor, as well as collecting and

providing to the Auditor in good order all the documents required to carry out the audit, including:

- 10.2.1 Bank statements for the AML/CFT audit period;
- 10.2.2 AML/CTF compliance manual;
- 10.2.3 Self \ Risk Assessment Report;
- 10.2.4 Latest Annual Compliance Report filed with the VFIU;
- 10.2.5 Pre-Audit Questionnaire
- 10.2.6 Detail of trainings conducted during the AML/CFT audit period, if any;
- 10.2.7 Copies of all reports filed with the VFIU over the AML/CFT audit period;
- 10.2.8 Access to correspondence file between the Reporting Entity and the VFIU.
- 10.2.9 High level review of the business of the Reporting Entity.

10.4 Following receipt of all information mentioned in Clause 13.3, the Auditor will review it and design various tests and select samples to audit the AML/CTF reporting entity compliance with the Act.

10.5 Once all documents have been collected and reviewed, the auditor will compile an Audit Report that shall include:

- 13.5.1 Identification of specific risk categories;
- 13.5.2 Independent review of AML&CTF processes;
- 13.5.3 Identification and understanding of vulnerabilities;
- 13.5.4 Potential or suggested mitigative measures;
- 13.5.4 Evaluation of the results with a weighted approach
- 13.5.4 Suggested corrective actions, if any, and conclusion;

10.6 Finally, the independent Auditor shall deliver the report to the Director(s) and Compliance Officer(s) of The Company, who shall then forward the report to the VFIU.

11. Systems to re-assess risk.

11.1. The Company will continue to review all areas of its business to identify potential ML/TF risks that may not be covered in the procedures described above. The additional areas of ML/TF risks are in respect of new products, services, distribution channels and developing technologies.

11.2. Additional procedures to address these ML/TF risks are as follows:

11.2.1. Chief Compliance Officer will be consulted by any person having responsibility for a new service or method of delivery or new technology ("the project manager") at design stage or prior to the introduction of the new service, delivery method or technology. He will be required to advise on the ML/TF risk factors which are to be considered having regard to:

- 11.2.1.1. the target market (customer type);
- 11.2.1.2. the service features;
- 11.2.1.3. foreign jurisdictional features / offerings;
- 11.2.1.4. any electronic access to / the delivery method of the service;
- 11.2.1.5. the business structure and process.

11.2.2. The Chief Compliance Officer or appointed responsible AML and CTF Compliance Officer will, in consultation with the project manager undertake the risk

- assessment and formulate the controls and systems to manage any ML/TF risks.
- 11.2.3. The Chief Compliance Officer or appointed responsible AML and CTF Compliance Officer will review the AML and CTF Program, policies, and procedures to ensure that any new ML/TF risks are identified in the AML and CTF Program and amendments to the AML and CTF Program are made. All amendments will require Board approval.
- 11.2.4. The Chief Compliance Officer or appointed AML and CTF Compliance Officer will formulate staff awareness and training programs in respect of the change to ML/TF risks and will oversee the delivery of training programs.
- 11.2.5. All records relevant to the risk assessment, addendums to the AML and CTF Program and the training programs are to be retained.
- 11.2.6. The Chief Compliance Officer or appointed AML and CTF Compliance Officer will ensure that any government or FATF findings concerning the approach to money laundering and terrorism financing prevention in particular countries or jurisdictions, is assessed and appropriate amendments made to the AML and CTF Program. Furthermore, all compliance procedures will be made and communicated to all Representatives.

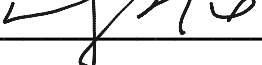
12. Confidentiality, Security and Protection.

- 12.1. The Company, its Officers and employees shall preserve the confidentiality of all information communicated and documents provided by its clients or potential clients, as well as their privacy, except where the Company is required by the law to report to relevant authorities any suspected illegal activities by clients, in adherence to sections 40AA, 40A, and 40B of the AML & CTF Act No. 13 of 2014 and subsequent amendments.
- 12.2. The Company shall ensure that its IT systems and internal procedures are secure against data leaks and shall take any other measure to protect the confidentiality of its clients or potential clients.
- 12.3. Any actual or suspected breach of Confidentiality, Privacy, Security or Protection shall be communicated immediately to the Compliance Officer(s).

Names of Compliance Officers (see Section 4.8 of this Policy)

Function	Name	Date of Appointment
Alternate Compliance officer	Yan ZHONG	June 14 th 2023
Compliance Officer	Jianshu ZHANG	January 1 ST 2024

This policy was approved by Mr. Wenlong ZHU, director of The Company, on the 26th day of February 2024.

Signature  _____